

Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 0 848 315 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
17.06.1998 Bulletin 1998/25

(51) Int Cl.⁶: G06F 1/00

(21) Application number: 97309424.6

(22) Date of filing: 21.11.1997

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(72) Inventor: Angelo, Michael F.
Houston, Texas 77068 (US)

(74) Representative: Brunner, Michael John et al
GILL JENNINGS & EVERY
Broadgate House
7 Eldon Street
London EC2M 7LH (GB)

(30) Priority: 13.12.1996 US 766267

(71) Applicant: Compaq Computer Corporation
Houston Texas 77070 (US)

(54) **Securely generating a computer system password by utilizing an external encryption algorithm**

(57) A method for generating system passwords derived from an external encryption algorithm and plain text user passwords entered during a secure power-on procedure. At some point during the secure power-up procedure, the computer system checks for the presence of an external token or smart card that is coupled to the computer through specialized hardware. The token or smart card is used to store an encryption algorithm furnished with an encryption key that is unique or of limited production. Following detection of the external token, the computer user is required to enter a user password. The user password is encrypted using the encryption algorithm contained in the external token, thereby creating a system password. The system password is then compared to a value stored in secure memory. If the two values match, the power-on sequence is completed and the user is allowed access to the computer system or individually secured resources. The two-piece nature of the authorization process requires the presence of both the user password and the external token in order to generate the system password.

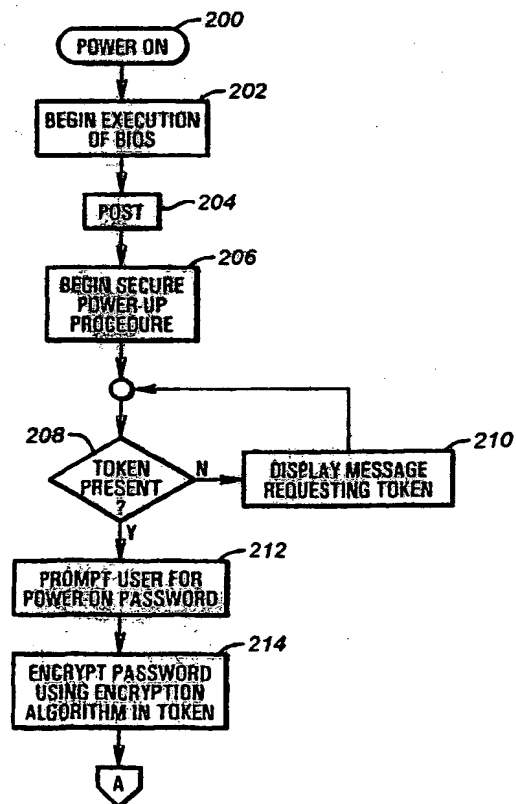


FIG. 2A

EP 0 848 315 A2

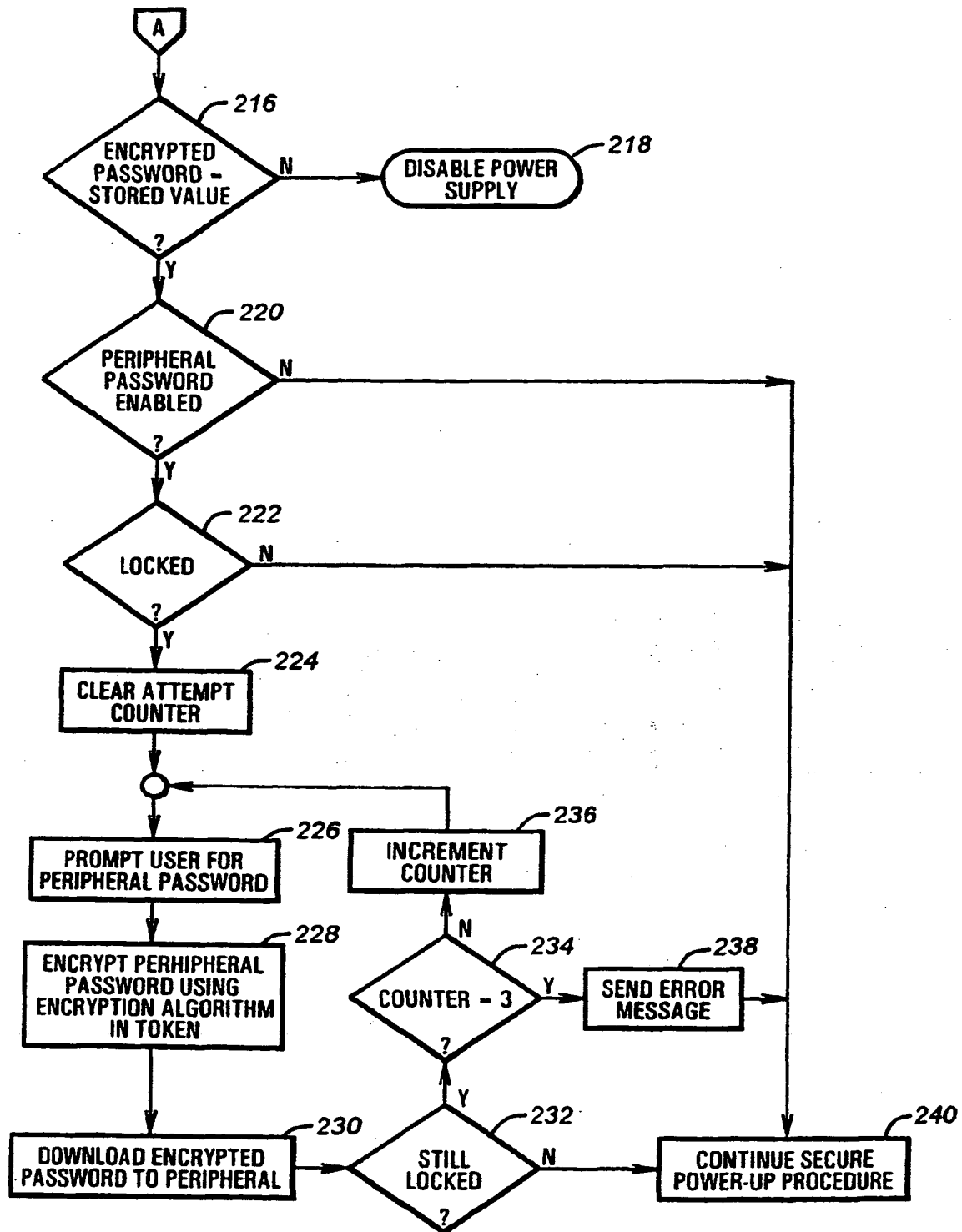


FIG. 2B

Description

The invention relates to security in a computer system, and more particularly to a method for generating system passwords derived from an external encryption algorithm and plain text passwords entered during a secure power-on procedure.

Large amounts of money are invested by companies and individuals to purchase computer hardware and software, and even more money is spent developing the information contained in data files such as text documents and spreadsheets. Protecting these investments can be critical to the success and reputation of a business. Public accounts of the exploits of computer "hackers" -- as malicious code-breakers or eavesdroppers are sometimes called -- have therefore focused and magnified corporate desires for more secure communications and better methods to protect data. The scope of the problem is undoubtedly even more serious than reported, given the reluctance of many businesses to report security breaches. As a result, security conscious users are requesting that security and integrity features be incorporated into their computers to restrict access to data contained on hard drives, as well as information contained in other critical system components.

One known approach to security involves encryption or cryptography. Cryptography is typically used to protect both data and communications. Generally, the original message or data item is referred to as "plain text", while "encryption" denotes the process of disguising or altering a message in such a way that its substance is not readily discernable. An encrypted message is called "ciphertext". Ciphertext is returned to plain text by an inverse operation referred to as "decryption". Encryption is typically accomplished through the use of a cryptographic algorithm, which is essentially a mathematical function. There are many types of cryptographic algorithms, providing varying levels of security.

The most common cryptographic algorithms are key-based, where special knowledge of variable information called a "key" is required to decrypt ciphertext. There are two prevalent types of key-based algorithms: "symmetric" (also called secret key or single key algorithms) and "public key" (also called asymmetric algorithms). The security in these algorithms is centered around the keys -- not the details of the algorithm itself. This makes it possible to publish the algorithm for public scrutiny and then mass produce it for incorporation into security products.

In most symmetric algorithms, the encryption key and the decryption key are the same. This single key encryption arrangement is not flaw-free. The sender and recipient of a message must somehow exchange information regarding the secret key. Each side must trust the other not to disclose the key. Further, the sender must generally communicate the key via another media (similar to a bank sending the personal identification

number for an ATM card through the mail). This arrangement is not practical when, for example, the parties interact electronically for the first time over a network. The number of keys also increases rapidly as the number of users increases.

With public key algorithms, by comparison, the key used for encryption is different from the key used for decryption. It is generally very difficult to calculate the decryption key from an encryption key. In typical operation, the "public key" used for encryption is made public via a readily accessible directory, while the corresponding "private key" used for decryption is known only to the recipient of the ciphertext. In an exemplary public key transaction, a sender retrieves the recipient's public key and uses it to encrypt the message prior to sending it. The recipient then decrypts the message with the corresponding private key. It is also possible to encrypt a message using a private key and decrypt it using a public key. This is sometimes used in digital signatures to authenticate the source of a message.

One problem with public key algorithms is speed. Public key algorithms are typically on the order of 1,000 times slower than symmetric algorithms. This is one reason that secure communications are often implemented using a hybrid cryptosystem. In such a system, one party encrypts a random "session key" with the other party's public key. The receiving party recovers the session key by decrypting it with his/her private key. All further communications are encrypted using the same session key (which effectively is a secret key) and a symmetric algorithm.

The number of cryptographic algorithms is constantly growing. The two most popular are DES (Data Encryption Standard) and RSA (named after its inventors -- Rivest, Shamir, and Adleman). DES is a symmetric algorithm with a fixed key length of 56 bits. RSA is a public key algorithm that can be used for both encryption and digital signatures. DSA (Digital Signature Algorithm) is another popular public key algorithm that is only used for digital signatures. With any of these algorithms, the relative difficulty of breaking an encrypted message by guessing a key with a brute force attack is proportional to the length of the key. For example, if the key is 40 bits long, the total number of possible keys (2^{40}) is about 110 billion. Given the computational power of modern computers, this value is often considered inadequate. By comparison, a key length of 56 bits provides 65,636 times as many possible values as the 40 bit key.

While much attention has been given to protecting communications and data as they are transmitted via internal networks (intranets) and external networks (such as the Internet), few security improvements have focused on the hardware itself. One known method of offering limited access to hardware and the data it contains is by the use of passwords. A password is typically stored in battery-backed CMOS RAM memory. Before the user is allowed access to the computer or secured computer resources, the user is required to enter a

password. Once a password is entered, the computer's power-on routines compares the password to the password in CMOS memory and, if they match, the user is allowed access.

A main disadvantage of this system is that certain forms of attack can bypass the CMOS memory because in many cases it is not read protected. To address this concern, the password can be encoded. Most encoding schemes can be reverse engineered by a sophisticated computer virus or malicious code, however, potentially leading to a costly security breach. Further, the CMOS memory could simply be disconnected from its battery, causing the loss of the password and any other contents.

Physical keys or tokens, such as those used to unlock a door, have also been used to permit access to a computer system. Like the password approach, this type of security is "one-piece" in nature, and is compromised if the key or token is stolen. Anyone possessing the key can gain access to the computer's data and is accorded the same level of access as the authorized user. Improvements in the security of and access to a computer system would be desirable, especially for network servers.

Briefly, a system according to the invention utilizes cryptographic security concepts in conjunction with password security to provide secure two-piece password or user verification. The verification process is carried out during a secure power-up procedure that verifies the integrity of system files prior to execution. At some point during the secure power-up procedure, the computer system checks for the presence of an external token or smart card that is coupled to the computer through hardware. The token or smart card is used to store an encryption algorithm furnished with an encryption key that is unique or of limited production.

Following detection of the external token, the computer user is required to enter a user password. Once entered, the user password is encrypted using the encryption algorithm contained in the external token, thereby creating a system password. The system password is compared to a value stored in secure memory. If the two values match, the power-on sequence is completed and the user is allowed access to the computer system or individually secured resources (which can be configured to require separate passwords). The two-piece nature of the authorization process is advantageous because if either the user password or the external token is misappropriated, it is of little value. Both pieces are required to generate the system password.

A better understanding of the present invention can be obtained when the following detailed description of the preferred embodiment is considered in conjunction with the following drawings, in which:

Figure 1 is a schematic block diagram of a computer system incorporating secure power-on capabilities in accordance with the present invention; and

Figures 2A and 2B are flowchart diagrams illustrating a secure power-on sequence incorporating two-piece user authentication according to the invention.

The following of our patents and applications are referred to in the description:

U.S. Patent No. 5,537,540, entitled "TRANSPARENT, SECURE COMPUTER VIRUS DETECTION METHOD AND APPARATUS", referred to as the "SAFESTART patent";

U.S. Patent Application Serial No. 08/396,343, entitled, "SECURITY CONTROL FOR A PERSONAL COMPUTER," filed on March 3, 1995;

U.S. Patent No. 5,375,243, entitled "HARD DISK PASSWORD SECURITY SYSTEM".

Referring first to Figure 1, a computer system S according to the present invention is shown. In the preferred embodiment, the system S incorporates two primary buses: a Peripheral Component Interconnect (PCI) bus P which includes an address/data portion and a control signal portion; and an Industry Standard Architecture (ISA) bus I which includes an address portion, a data portion, and a control signal portion. The PCI and ISA buses P and I form the architectural backbone of the computer system S.

A CPU/memory subsystem 100 is connected to the PCI bus P. The processor 102 is preferably the Pentium® processor from Intel Corporation, but could be an 80486 or any number of similar or next-generation processors. The processor 102 drives data, address, and control portions 116, 106, and 108 of a host bus HB. A level 2 (L2) or external cache memory 104 is connected to the host bus HB to provide additional caching capabilities that improve the overall performance of the computer system S. The L2 cache 104 may be permanently installed or may be removable if desired. A cache and memory controller 110 and a PCI-ISA bridge chip 130 are connected to the control and address portions 108 and 106 of the host bus HB. The cache and memory controller chip 110 is configured to control a series of data buffers 112. The data buffers 112 are preferably the 82433LX from Intel, and are coupled to and drive the host data bus 116 and a MD or memory data bus 118 that is connected to a memory array 114. A memory address and memory control signal bus is provided from the cache and memory controller 110.

The data buffers 112, cache and memory controller 110, and PCI-ISA bridge 130 are all connected to the PCI bus P. The PCI-ISA bridge 130 is used to convert signals between the PCI bus P and the ISA bus I. The PCI-ISA bridge 130 includes: the necessary address and data buffers, arbitration and bus master control logic for the PCI bus P, ISA arbitration circuitry, an ISA bus controller as conventionally used in ISA systems, an IDE (intelligent drive electronics) interface, and a DMA con-

troller. A hard disk drive 140 is connected to the IDE interface of the PCI-ISA bridge 130. Tape drives, CD-ROM devices or other peripheral storage devices (not shown) can be similarly connected.

In the disclosed embodiment, the PCI-ISA bridge 130 also includes miscellaneous system logic. This miscellaneous system logic contains counters and activity timers as conventionally present in personal computer systems, an interrupt controller for both the PCI and ISA buses P and I, and power management logic. Additionally, the miscellaneous system logic may include circuitry for a security management system used for password verification and to allow access to protected resources as described more fully below.

The PCI-ISA bridge 130 also includes circuitry to generate a "soft" SMI (System Management Interrupt), as well as SMI and keyboard controller interface circuitry. The miscellaneous system logic is connected to the flash ROM 154 through write protection logic 164. As discussed below, separate enable/interrupt signals are also communicated from the PCI-ISA bridge 130 to the power supply 180 and the hard drive 140. Preferably, the PCI-ISA bridge 130 is a single integrated circuit, but other combinations are possible.

A series of ISA slots 134 are connected to the ISA bus I to receive ISA adapter cards. A series of PCI slots 142 are similarly provided on the PCI bus P to receive PCI adapter cards.

A video controller 165 is also connected to the PCI bus P. Video memory 166 is used to store graphics data and is connected to the video graphics controller 165 and a digital/analog converter (RAMDAC) 168. The video graphics controller 165 controls the operation of the video memory 166, allowing data to be written and retrieved as required. A monitor connector 169 is connected to the RAMDAC 168 for connecting a monitor 170.

A network interface controller (NIC) 122 is also connected to the PCI bus P. Preferably, the controller 122 is a single integrated circuit that includes the capabilities necessary to act as a PCI bus master and slave, as well as circuitry required to act as an Ethernet interface. Attachment Unit Interface (AUI) and 10 base-T connectors 124 are provided in the system S, and are connected to the NIC 122 via filter and transformer circuitry 126. This circuitry forms a network or Ethernet connection for connecting the computer system S to a local area network (LAN).

A combination I/O chip 136 is connected to the ISA bus I. The combination I/O chip 136 preferably includes a real time clock, two UARTS, a floppy disk controller for controlling a floppy disk drive 138, and various address decode logic and security logic to control access to an internal or external CMOS/NVRAM memory (not shown) and stored password values. Further details of contemplated uses of the NVRAM memory are provided below. Additionally, a control line is provided to the read and write protection logic 164 to further control access to the flash ROM 154. Serial port connectors 146 and

parallel port connector 132 are also connected to the combination I/O chip 136.

An 8042, or keyboard controller, is also included in the combination I/O chip 136. The keyboard controller is of conventional design and is connected in turn to a keyboard connector 158 and a mouse or pointing device connector 160. A keyboard 159 is connected to the computer system S through the keyboard connector 158.

A buffer 144 is connected to the ISA bus I to provide an additional X-bus X for various additional components of the computer system S. A flash ROM 154 receives its control, address and data signals from the X-bus X. Preferably, the flash ROM 154 contains the BIOS information for the computer system and can be reprogrammed to allow for revisions of the BIOS.

In the disclosed embodiment, the computer system S contains circuitry for communicating with a removable cryptographic token 188. The precise physical nature of the token 188 is not considered critical to the invention. The token can take many forms, such as a Touch Memory™ device supplied by Dallas Semiconductor, Inc., a smart card, or an encryption card. Preferably, the token 188 is easily decoupled from the computer system S and easily transportable by the token bearer. The token 188 contains at least one of a variety of encryption algorithms (such as DES, Blowfish, elliptic curve-based algorithms, etc.). Although the base algorithm can be the same in each token 188, it is preferable that the encryption key be different in each token 188. Ideally, the token 188 is capable of communicating digitally with the computer system S during momentary contact with or proximity to the computer system S. The token 188 of the disclosed embodiment is capable of storing the encryption algorithm in a non-volatile manner and can be permanently write-protected to discourage tampering.

In the disclosed embodiment of the invention, the circuitry used for establishing a communication link between the token 188 and the computer system S consists of a probe 186 connected to a COM or serial port adapter 184. The port adapter 184 is connected to the RS232 connector 146. In operation, the token 188 is detachably received by the probe 186. The probe 186 includes circuitry for reading and writing memory in the token 188, and can be fully powered through the RS232 connector 146. In addition, the probe 186 includes presence detector circuitry for ascertaining the presence of a token 188.

An additional feature of the computer system S is a System Management Mode (SMM), which is generally known to those skilled in the art. It is also noted that Figure 1 presents an exemplary embodiment of the computer system S and it is understood that numerous other effective embodiments could readily be developed as known to those skilled in the art.

Referring now to Fig. 2A and 2B, an exemplary power-on sequence incorporating two-piece user verification according to the invention is shown. The sequence builds upon a secure power-up procedure, such as that

described in the SAFESTART patent. Briefly, this invention reduces the administrative requirements of earlier techniques. A reserved non-DOS hard disk partition is used to pre-boot the computer system and provide a secure environment from which to verify files. Upon power-up or reset, the computer performs the power-on self test (POST), during which it checks a SAFESTART track by comparing its hash value to a value stored in NVRAM. If the integrity of the SAFESTART track is verified, the first "SAFESTART" routine is loaded into memory and executed.

The SAFESTART routine first checks the master boot record and boot sectors of the hard disk. This verification captures a large majority of viruses and is performed before any code residing in those areas is executed, thus preventing the spread of any discovered viruses. Further checks are performed on SAFESTART files before each is executed. Eventually, system files and any additional designated user files are verified. Since the computer system was booted from an atypical partition, the drives are remapped to account for the shift in logical disk drive addressing. When the verification process is completed, SAFESTART files are cleaned up, a latch is set to prevent unauthorized modification of the initial hash values, and control is returned to the BIOS to boot the user operating system. Thus, a computer system implemented according to the SAFESTART patent insures that designated software and passwords are trustworthy following a power-up cycle.

As shown in Figure 2A, when power to the computer system S is initially applied or the system undergoes a cold restart, the POWER-ON sequence 200 is commenced. In the first step 202 of the POWER-ON sequence 200 the computer system S begins executing from BIOS ROM. The BIOS is preferably stored in flash ROM 154 and contains low level programming for booting the operating system, and an interrupt handler for accessing the hard drive 140. Control then proceeds to step 204 where the computer system S performs a power-on self test (POST) to determine if all system hardware is operating properly.

Following additional power-on steps (optional), control next proceeds to step 206 for commencement of a secure power-up procedure such as that described in the SAFESTART patent. In the preferred embodiment, operating sequences for the secure power-up procedure are configured as an option ROM and located in the option ROM address space in a conventional manner. Preferably, the operating sequences are provided as the last option ROM in order to allow any other option ROM's to be installed at the outset. The system BIOS executes this portion of the secure power-on sequence as a part of its scan for option ROMs, which are executed when encountered in POST. This arrangement requires address decoding for the power-on sequence, but also simplifies distribution into a family of computer systems. Alternatively, the power-on sequence could be implemented as a direct call from the

BIOS, rather than an option ROM call.

Control next proceeds to step 208 to determine if a token 188 containing an encryption algorithm is present. If the aforementioned presence detection circuitry determines that a token is not present, control loops to step 210 to display a message requesting that the user provide a token 188. When a token 188 is present as determined in step 208, control passes to step 212 where the user is prompted to enter a plain text power-on password. As an alternative to a memorized value, the plain text password could be generated with the aid of biometrics. For example, a scanned fingerprint could be converted into a plain text password value.

Control next proceeds to step 214 and the plain text password entered by the user is encrypted using the encryption algorithm provided by the external token 188. The encrypted plain text password effectively becomes the system password, and is referred to as such throughout this specification. The encryption algorithm that is utilized can take many forms, including DES, RSA, DSA, RC2, RC4, Blowfish, IDEA, 3-WAY, and MDC among others. Ideally, the algorithm in each token 188 is enabled by an encryption key that is unique or of limited production, such that it is impractical or impossible to circumvent the verification process by using a substitute token.

It is contemplated that the actual encryption process could be carried out by the token 188 itself. In this embodiment of the invention, the plain text password is transmitted to the token 188 through the RS232 connector 146 or alternate connection port. The token 188 then performs the encryption procedure using its stored encryption algorithm and associated encryption key. Following the encryption process, the encrypted password is returned to the computer system S via the RS232 connector 146.

In an alternate embodiment of the invention, the encryption algorithm is downloaded into secure computer memory. After the user password has been entered, the encryption process is then performed by the computer system S. In this embodiment of the invention, it is desirable that the encryption algorithm be erased from the computer memory after completion of the encryption process and while the computer system S is still in the secure power-on period. This step prevents the encryption algorithm from being surreptitiously obtained from memory after the secure power-on period.

Following encryption of the password, control proceeds to step 216 of Figure 2B, and the encrypted password value (i.e. the system password) is compared to a stored value. The stored value is preferably located in protected/locked NVRAM or Flash ROM 154, or in some other secure memory such as that disclosed in the previously referenced U.S. Patent Application Serial No. 08/396,343 "SECURITY CONTROL FOR A PERSONAL COMPUTER." That reference describes a security system in which system ROM provides a password at power-on to a security device (hereinafter referred to as

the "black box" security device). The black box security device controls access to various secured resources of the computer system, such as the flash ROM 154 or any designated hardware peripheral devices. Once a password has been downloaded to the black box security device, a command to protect secured resources is issued to the security device. The command prevents unauthorized access to any of the secured resources. To access a secured resource, the user must thereafter provide the correct password to the black box security device. The security device can only verify--but does not divulge--the password, thereby enhancing system security. A multitude of passwords or other information can be protected with the black box security device.

Returning to Figure 2B, if the encrypted password and the stored value are not equal as determined in step 216, control proceeds to step 218 and the power supply 180 is disabled. The resulting delay associated with rebooting the computer system discourages brute force attacks against the user password in situations where the external token has been misappropriated.

Several other options are available at this point. In one contemplated embodiment of the invention, the core components needed to boot the computer system S are powered by one supply voltage (V_{DC1}), while other secured components are powered by a second supply voltage (V_{DC2}). Devices powered by the second supply signal might include bay door/case locks and mass storage devices. Under this arrangement, the second power supply signal is initially disabled, but is turned on following detection of a valid system password. The system password used for this operation could be the same password generated in step 214, or a separate password that is generated at a later point (even outside of the secure power-up procedure). By requiring entry of a valid system password before enabling power to peripheral devices or unlocking bay door/case locks, the possessor of a stolen computer will usually be forced to physically damage the computer casing before gaining access to secured resources. The value of stolen computer equipment is thereby reduced, and computer theft is discouraged.

As shown in Figure 2B, the secure power-up procedure can also include steps that provide password security for specified peripheral devices. In the disclosed embodiment of the invention, the procedure for gaining access to a single secured peripheral device begins at step 220 following detection of a valid system password in step 216. In step 220, the specified peripheral device is polled to determine if it is password enabled.

One device that could be secured in accordance with the invention is a disk drive such as that described in the previously referenced U.S. Patent No. 5,375,243, "HARD DISK PASSWORD SECURITY SYSTEM." In a disk drive according to that invention, unauthorized access is prevented by placing an access password on the disk drive itself. When the computer system is powered up, the disk drive unit is in a LOCKED state and de-

mands the password before access is allowed. No access to the disk drive -- other than to wipe all of the data from the drive or to check the drive's status -- is permitted until the password on the disk drive is received. If the user attempts to gain access to the disk drive by removing the drive from the original computer and placing it in another system, the disk drive remains inaccessible. Because the password is located on a secure portion of the disk drive instead of in the system CMOS, the disk will remain LOCKED regardless of the computer system in which it is operating. Circuitry is also included for preventing an unauthorized user from bypassing the security system by simply swapping the firmware controlling the disk drive.

If the disk drive or other secured peripheral is password enabled as determined in step 220, control passes to step 222 and the peripheral is examined to determine if it is locked. Ideally, the peripheral is locked each time power to the computer system S is cycled. If the specified peripheral device is not locked (i.e. the peripheral password is the same as the password generated in step 214), or if the peripheral device is not password enabled, control proceeds to step 240 and any remaining steps in the secure power-up procedure are completed.

If the peripheral device is locked, control proceeds to 224 and an optional attempt counter is cleared. Control then passes to step 226 and the computer user is prompted to enter a plain text password. Next, in step 228, the plain text password is encrypted with the encryption algorithm stored in the token 188 to generate a "peripheral" password. As discussed above, the encryption process can be completed in secure computer system S memory or in the token 188 itself.

In the disclosed embodiment of the invention, control next passes to step 230 where the peripheral password is downloaded to the secured peripheral for comparison to a value stored in the peripheral device's memory. The peripheral device remains in a locked state if the two values do not match. By storing the valid encrypted password value in the peripheral device's local memory, the peripheral device can be moved to another computer system and yet require the same user password and token 188 for access. Alternatively, the stored value could be maintained in secure computer system S memory such as the aforementioned black box security device.

After the peripheral password is downloaded and compared to a stored value, the peripheral device is polled in step 232 to determine if it is still locked. If it is not locked, control passes to step 240 and the secure power-up procedure is completed. If the peripheral device is still locked, control instead passes to step 234 to determine if the maximum number of allowed attempts (shown as 3) at generating the correct peripheral password has been reached. If not, the attempt counter is incremented in step 236 and control then returns to step 226 where the user is prompted to enter a new plain text

password. If the maximum number of attempts is reached, control proceeds to step 238 for display of an optional error message. Control then passes to step 240 and the secure power-up procedure is completed.

It should be observed that in each of the embodiments of the invention described above, the user authentication or password verification process is two-piece in nature. If either the user password or the external token is misappropriated, it is of little value. Both pieces are required to generate the system password. In addition, the scope of the invention not considered to be limited to the disclosed secure power-up procedure. Likewise, the precise ordering of the power-up steps is not considered critical to the invention.

Thus, a method has been described for generating system passwords derived from an external encryption algorithm and plain text user passwords entered during a secure power-on procedure. An external token or smart card is used to store the encryption algorithm, which is furnished with an encryption key that is unique or of limited production. Following detection of the external token, the computer user is prompted to enter a user password. The user password is then encrypted using the encryption algorithm contained in the external token, thereby creating a system password. The system password is compared to a value stored in secure memory. If the two values match, the power-on sequence is completed and the user is allowed access to the computer system or individually secured resources. The two-piece nature of the authorization process requires the presence of both the user password and the external token in order to generate the system password.

The foregoing disclosure and description of the invention are illustrative and explanatory thereof, and various changes in the size, shape, materials, components, circuit elements, wiring connections and contacts, as well as in the details of the illustrated circuitry and construction and method of operation may be made without departing from the spirit of the invention.

Claims

1. A method for securely generating a system password in a computer system incorporating circuitry for communicating with an external token that includes a cryptographic algorithm and an encryption key, the computer system further incorporating a secure power-on process or other secure operating mode, the method comprising the steps of:

providing a user password to the computer system;
communicatively coupling the external token to the computer system;
providing the user password to the cryptographic algorithm stored in the token; and
encrypting the user password with the crypto-

graphic algorithm and the encryption key to produce a system password.

2. The method of claim 1, further comprising the steps of:
 - comparing the system password with a stored system password value; and
 - permitting further computer system operations if the system password matches the stored system password value.
3. The method of claim 1, wherein said step of providing a user password to the computer system is performed while the computer system is in a secure period of operation.
4. The method of claim 3, wherein the secure period of operation includes a secure power-up procedure.
5. The method of claim 1, wherein said step of encrypting the user password with the cryptographic algorithm and the encryption key occurs in the token.
6. The method of claim 5, further comprising the step of communicating the system password from the token to the computer system.
7. The method of claim 1, wherein said step of providing the user password to the cryptographic algorithm comprises downloading both the cryptographic algorithm and the user password to secure computer memory, and wherein said step of encrypting the user password with the cryptographic algorithm and the encryption key occurs in secure computer memory.
8. The method of claim 1, wherein the token is a smart card.
9. The method of claim 1, wherein the token is a Touch Memory™ device.
10. The method of claim 1, wherein the encryption key is unique or of limited production.
11. The method of claim 1 wherein the cryptographic algorithm is based on secret key technology.
12. The method of claim 11 wherein the cryptographic algorithm is DES.
13. The method of claim 1 wherein the cryptographic algorithm is an asymmetric algorithm.
14. The method of claim 13 wherein the cryptographic algorithm is RSA.

15. The method of claim 13 wherein the cryptographic algorithm is an elliptic-curve based algorithm.
16. A computer system having security capabilities that operate in conjunction with an external token containing a cryptographic algorithm and an encryption key, comprising: 5
- a system bus;
 - a processor coupled to said system bus; 10
 - communication circuitry coupled to said processor for communicating with the external token; and
 - power-on code stored in a processor readable medium for causing the processor, on power-on, to perform the steps of: 15
 - receiving a user password;
 - providing the user password to the external token; and
 - receiving a system password from the external token, wherein the system password is an encrypted version of the user password. 20
17. The computer system of claim 16, wherein said power-on code is executed during a secure power-on procedure. 25
18. The computer system of claim 16, wherein said power-on code further causes the processor to allow further computer system operation if the system password matches a stored system password value. 30
19. The computer system of claim 16, wherein said power-on code causes the processor to provide the user password to the external token without retrieving the cryptographic algorithm or the encryption key from the token. 35
20. The computer system of claim 16, wherein the token is a smart card. 40
21. The computer system of claim 16, wherein the token is a Touch Memory™ device. 45
22. The computer system of claim 16, wherein the encryption key is unique or of limited production.
23. The computer system of claim 16 wherein the cryptographic algorithm is DES. 50

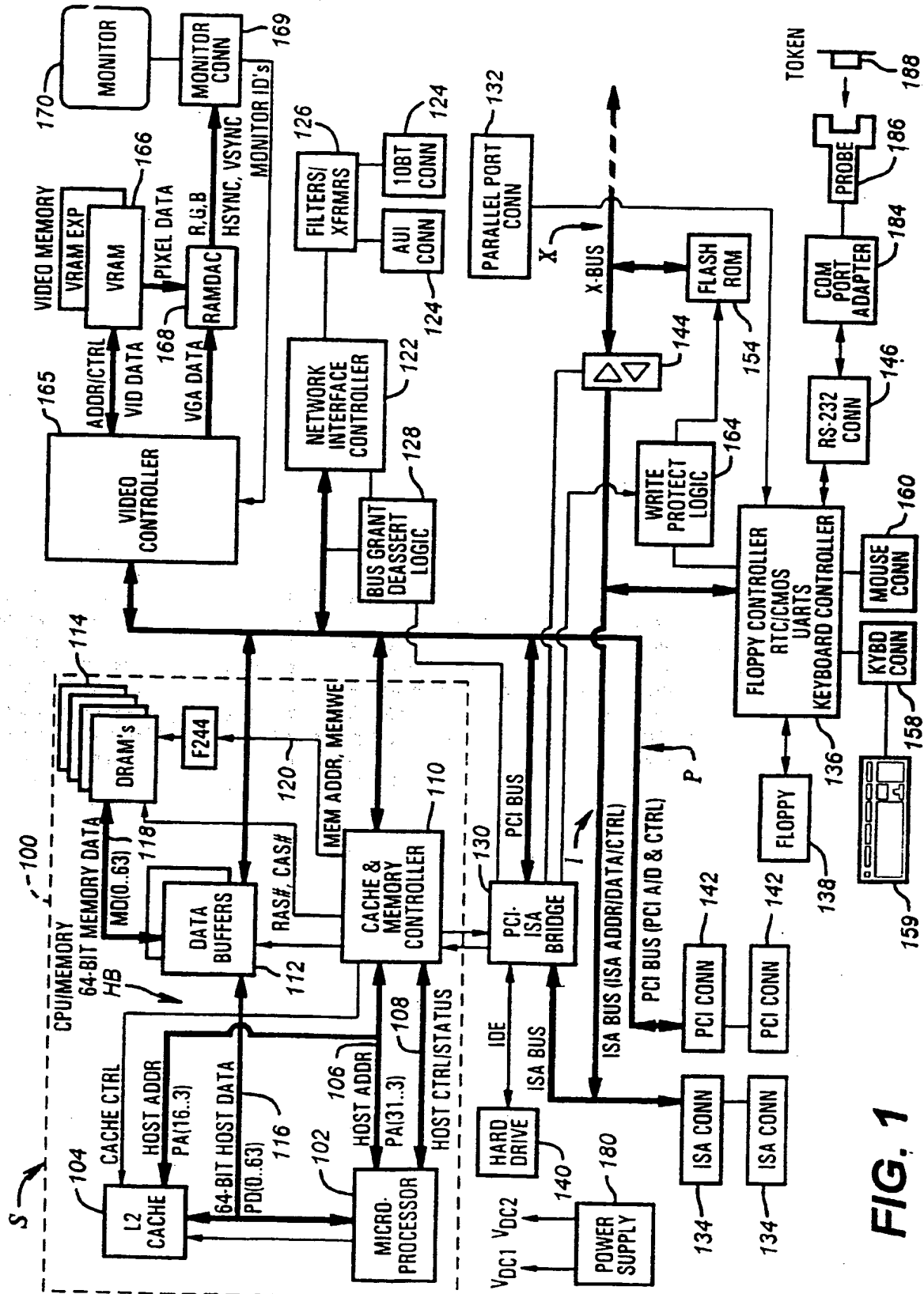
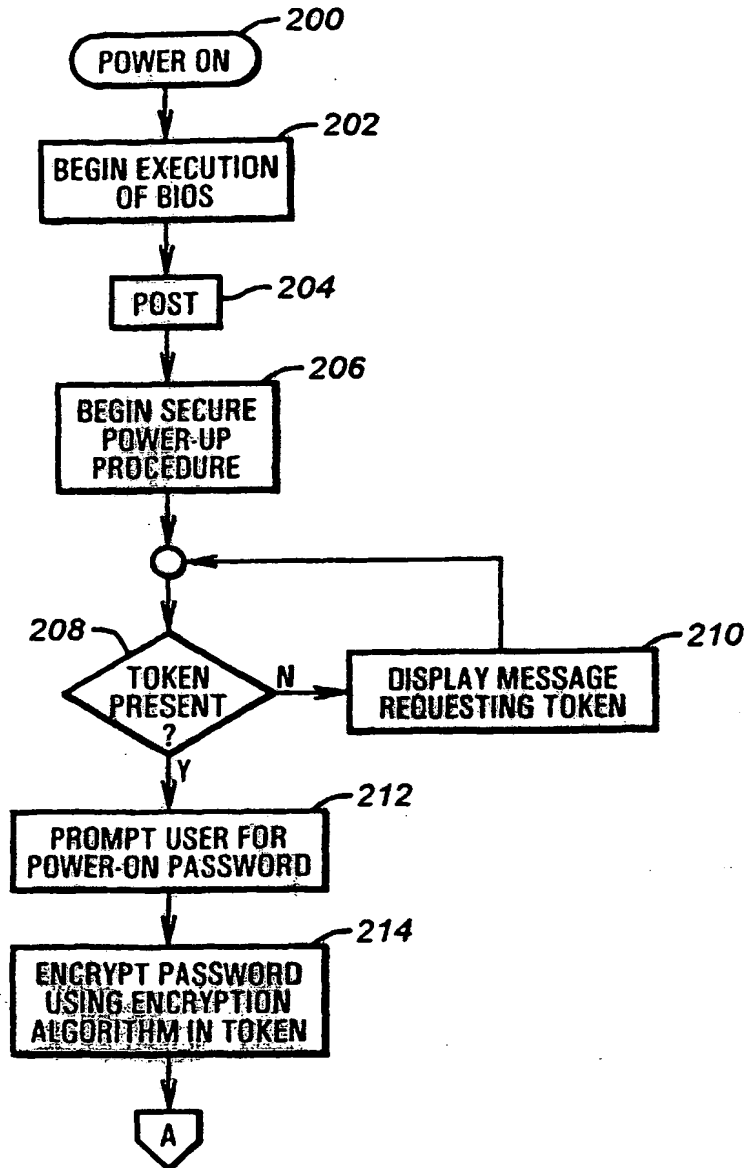


FIG. 1

**FIG. 2A**

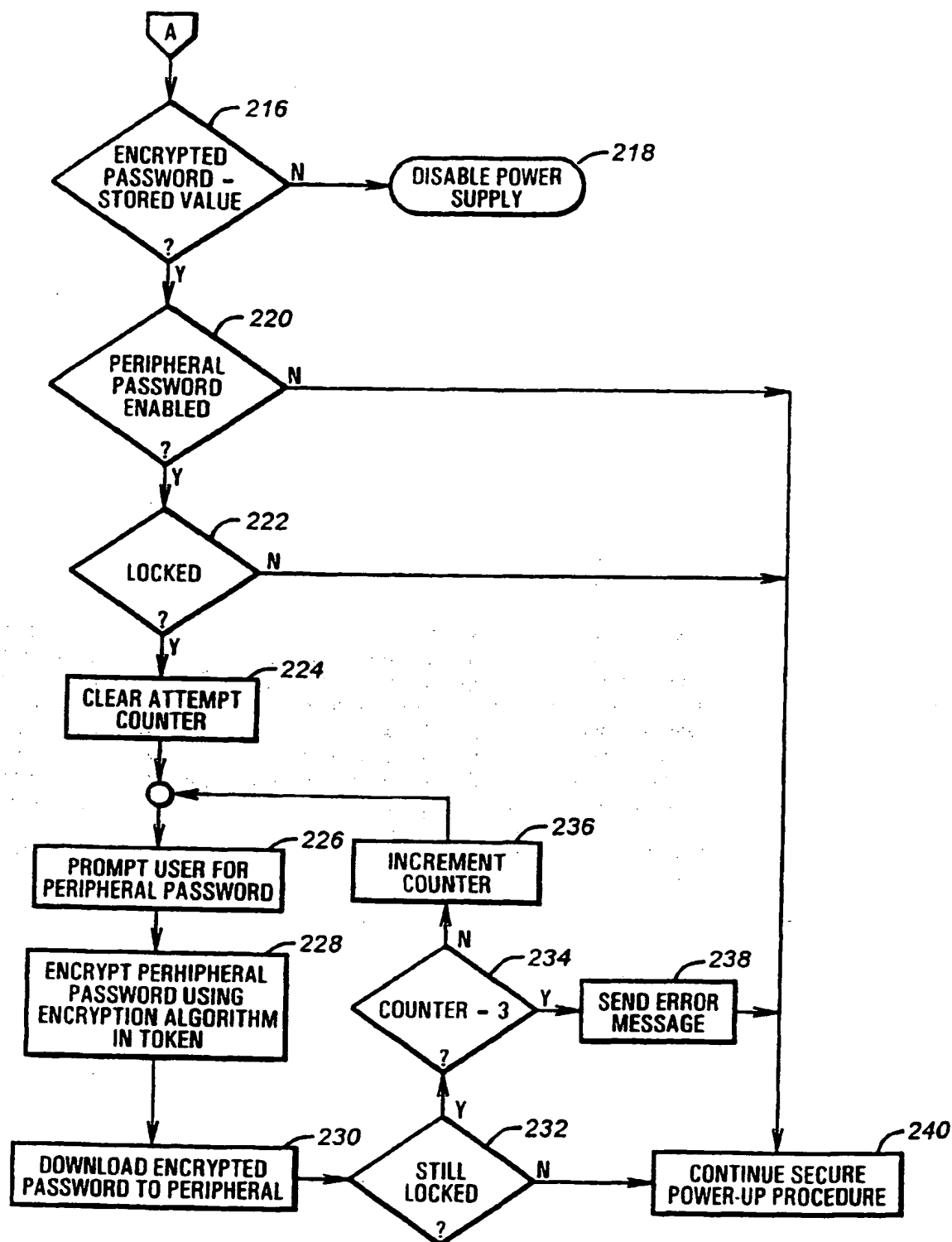


FIG. 2B

(19)



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 0 848 315 A3

(12)

EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
16.06.1999 Bulletin 1999/24

(51) Int Cl.⁶: **G06F 1/00**

(43) Date of publication A2:
17.06.1998 Bulletin 1998/25

(21) Application number: **97309424.6**(22) Date of filing: **21.11.1997**

(84) Designated Contracting States:
**AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
NL PT SE**
Designated Extension States:
AL LT LV MK RO SI

(72) Inventor: **Angelo, Michael F.**
Houston, Texas 77068 (US)

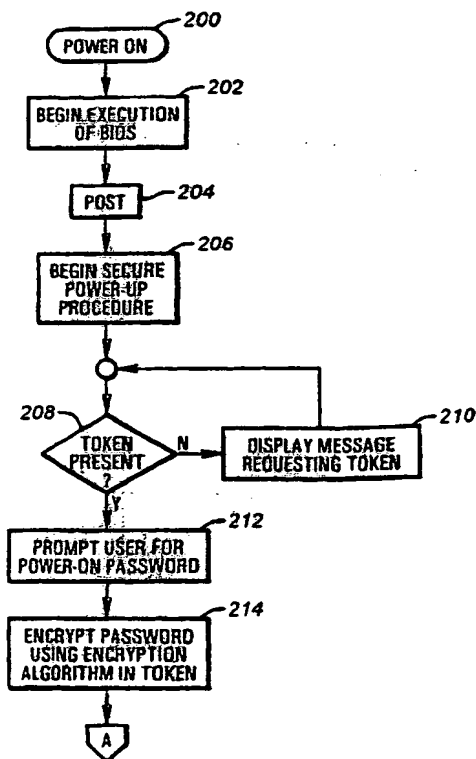
(74) Representative: **Brunner, Michael John et al**
GILL JENNINGS & EVERY
Broadgate House
7 Eldon Street
London EC2M 7LH (GB)

(30) Priority: **13.12.1996 US 766267**

(71) Applicant: **Compaq Computer Corporation**
Houston Texas 77070 (US)

(54) **Securely generating a computer system password by utilizing an external encryption algorithm**

(57) A method for generating system passwords derived from an external encryption algorithm and plain text user passwords entered during a secure power-on procedure. At some point during the secure power-up procedure, the computer system checks for the presence of an external token or smart card that is coupled to the computer through specialized hardware. The token or smart card is used to store an encryption algorithm furnished with an encryption key that is unique or of limited production. Following detection of the external token, the computer user is required to enter a user password. The user password is encrypted using the encryption algorithm contained in the external token, thereby creating a system password. The system password is then compared to a value stored in secure memory. If the two values match, the power-on sequence is completed and the user is allowed access to the computer system or individually secured resources. The two-piece nature of the authorization process requires the presence of both the user password and the external token in order to generate the system password.

**FIG. 2A**
EP 0 848 315 A3

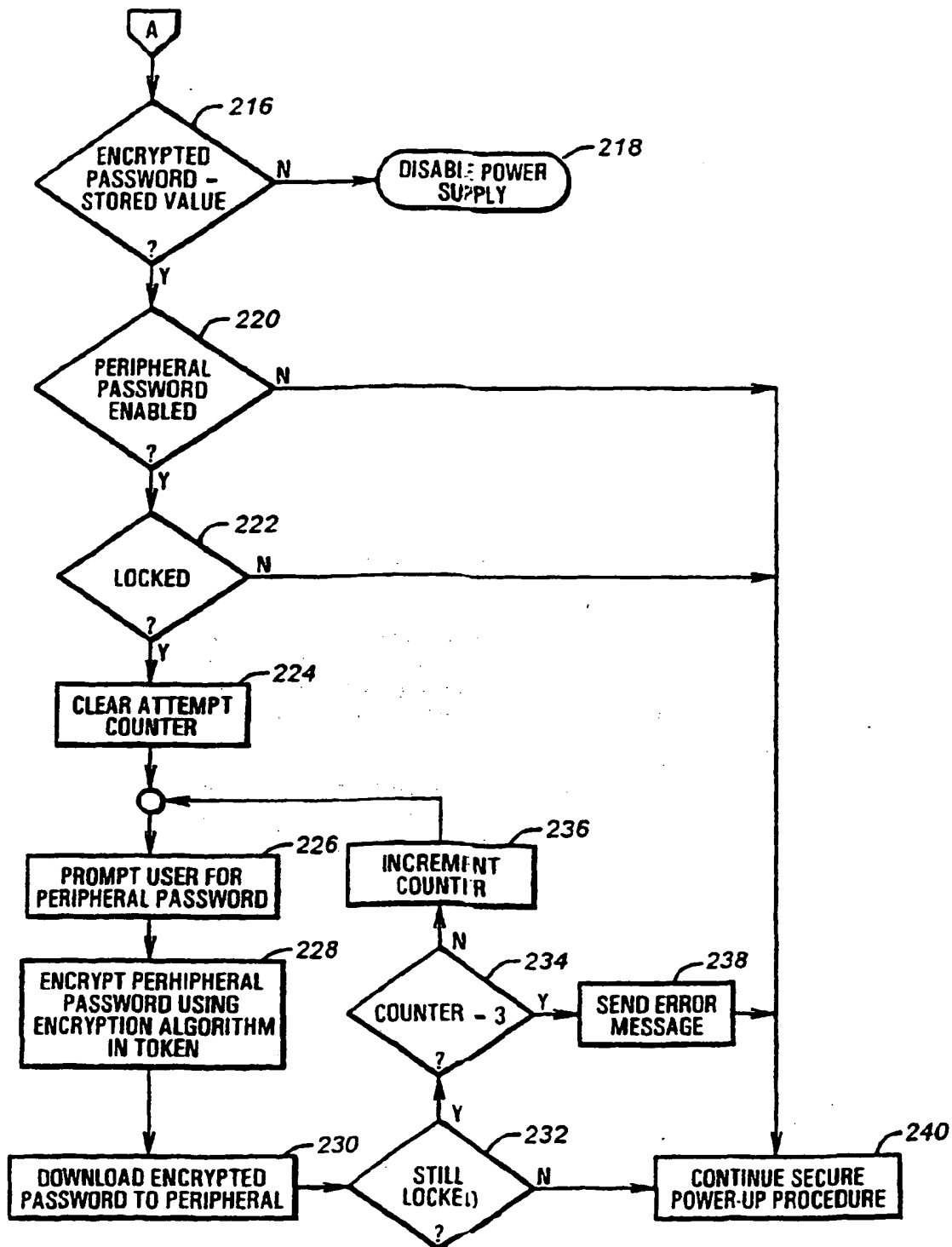


FIG. 2B



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 30 9424

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	US 5 146 499 A (GEFFROTIN BERNARD) 8 September 1992 * column 1, line 1 - column 4, line 25 * * column 6, line 41 - line 55 * * column 11, line 24 - column 12, line 4 *	1-12, 16-23	G06F1/00
Y	---	13-15	
Y	"BITS: A SMARTCARD PROTECTED OPERATING SYSTEM" COMMUNICATIONS OF THE ASSOCIATION FOR COMPUTING MACHINERY, vol. 37, no. 11, 1 November 1994, pages 66-70, 94, XP000485634 * the whole document *	13,14	
Y	MIYAJI A: "ELLIPTIC CURVES SUITABLE FOR CRYPTOSYSTEMS" IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS, COMMUNICATIONS AND COMPUTER SCIENCES, vol. E77-A, no. 1, 1 January 1994, pages 98-104, XP000439669 * the whole document *	15	
A	"JEWELRY FOR THE INFORMATION AGE" ELECTRONICS, vol. 244, no. 17, 18 September 1995, page 49 XP000535371 * the whole document *	9,21	
A	WO 95 24696 A (INTEGRATED TECH AMERICA : MOONEY DAVID M (US); WOOD DAVID E (US); K) 14 September 1995 -----		
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 28 April 1999	Examiner Powell, D
<p>CATEGORY OF CITED DOCUMENTS</p> <p>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p> <p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons s : member of the same patent family, corresponding document</p>			

EPO FORM 1503 03/82 (P4/C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 97 30 9424

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

28-04-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5146499 A	08-09-1992	FR 2653914 A	03-05-1991
		EP 0425053 A	02-05-1991
		JP 3152653 A	28-06-1991
WO 9524696 A	14-09-1995	US 5610981 A	11-03-1997
		AT 175505 T	15-01-1999
		AU 703856 B	01-04-1999
		AU 2092695 A	25-09-1995
		CA 2183759 A	14-09-1995
		CN 1146813 A	02-04-1997
		DE 69507129 D	18-02-1999
		EP 0748474 A	18-12-1996
		NZ 282954 A	24-11-1997

EPO FORM P459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82